KASPERSKY LAB

Kaspersky Mobile Security 7.0 Enterprise Edition

USER'S GUIDE

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

User's Guide

© Kaspersky Lab
http://www.kaspersky.com

Revision Date: August, 2009

Table of Contents

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION 5
1.1. Hardware and software requirements 6
1.2. Distribution Kit 6
1.3. Installing Kaspersky Mobile Security 6
1.3.1. Installing using the user's computer 7
1.3.2. Installing using an SMS message 7
1.4. Activating the application 8

CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS 9
2.1. Using the application 9
2.1.1. Starting the application 9
2.1.2. Graphical user interface 10
2.1.3. General settings 11
2.1.4. Anti-virus scan and protection 12
2.1.5. Using Quarantine 17
2.1.6. Using Anti-Spam 19
2.1.7. Using Anti-Thief 24
2.1.8. Updating the application bases 27
2.1.9. Updating the application operation settings 30
2.1.10. Using the Firewall module 31
2.1.11. Viewing report about the application operation 32
2.2. Uninstalling the application 33

CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE 36
3.1. Getting started 36
3.1.1. Starting the application 36
3.1.2. Graphical user interface 37
3.2. Anti-virus scan and Real-Time protection 38
3.2.1. On-demand scan 39
3.2.2. Real-time protection 41
3.2.3. Scheduled scan 42

3.3. Using Quarantine ... 43
3.4. Using Anti-Spam and Anti-Theft modules ... 44
3.4.1. Anti-Spam module ... 45
3.4.2. The Anti-Theft tab ... 48
3.5. Updating the application bases ... 51
3.6. Updating the application operation settings ... 53
3.7. Firewall ... 53
3.8. Viewing reports about the application operation ... 54
3.9. Uninstalling the application ... 55

APPENDIX A. KASPERSKY LAB ... 59

APPENDIX B. CRYPTOEX LLC ... 61

APPENDIX C. KASPERSKY LAB END USER LICENSE AGREEMENT ... 62

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Kaspersky Mobile Security 7.0 Enterprise Edition is designed to ensure protection of mobile devices running Symbian OS and Microsoft Windows Mobile against malware programs and unsolicited e-mail messages and performs the following functions:

- **Real-time protection** of the file system of the device - interception and scan of:
  - al incoming objects transmitted using wireless connections (IR port, Bluetooth) and EMS messages, during synchronization with the personal computer and downloading files using a browser;
  - files opened on the mobile device;
  - programs installed from the device's interface.
- **scanning of the file system's objects** on the mobile device or on the connected expansion cards by user's demand or according to the schedule;
- **reliable isolation of infected objects** in the quarantine storage;
- **updating of Kaspersky Mobile Security bases** used to scan for malware programs and delete dangerous objects.
- **blocking unwanted SMS messages**.
- **blocking access to or erasing user's data** in case of unauthorized actions with the device, as, for instance, theft.
- **protection of the mobile device at the network level**.

The user can use the capabilities providing flexible control of the Kaspersky Mobile Security operation settings, viewing the current anti-virus protection status and the event log in which the application's actions are recorded.

The application includes a menu system and support an easy-to-use user's interface.

Note

In case a detection of a malware program, Kaspersky Mobile Security can disinfect the infected object detected (if disinfection is possible), delete it or place it into the quarantine. In this case no copies of the object being deleted will be saved.

1.1. Hardware and software requirements

Kaspersky Mobile Security is designed for installation on mobile devices running one of the following operating systems:

- Symbian OS 9.1, 9.2 Series 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Distribution Kit

You can purchase Kaspersky Mobile Security via internet (the application distribution kit and documentation in the electronic form). Kaspersky Mobile Security can be also purchased in mobile communication offices. For more details contact you mobile communication operator.

1.3. Installing Kaspersky Mobile Security

Note

The installed Kaspersky Mobile Security is not intended for backup and restore.

The application is installed using a centralized installation using Kaspersky Administration Kit. The network Administrator can use one of the two methods of the application installation.

- installation using the user's computer;
- installation using an SMS message.

For more details about the remote installation of the application see Kaspersky Mobile Security 7.0 Enterprise Edition “Administrator’s Guide”.

1.3.1. Installing using the user’s computer

After you connect the mobile device to a computer included into the Administration Server logical network, *kmlisten.exe* utility window will open (see Figure 1). This utility is designed to ensure installation of Kaspersky Mobile Security 7.0 Enterprise Edition onto a mobile device.

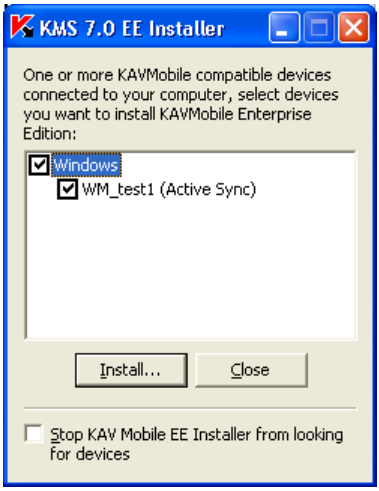
KMS 7.0 EE Installer
One or more KAVMobile compatible devices connected to your computer, select devices you want to install KAVMobile Enterprise Edition:
Windows
WM_test1 (Active Sync)
Install...
Close
Stop KAV Mobile EE Installer from looking for devices

Figure 1. **Kmlisten** utility

In order to install Kaspersky Mobile Security, perform the following actions:

using *kmlisten.exe* utility window, check the box next to the name of the device onto which you wish to install the application and press the **Install** button. The distribution kit for the application installation will be copied to your mobile device and started.

1.3.2. Installing using an SMS message

In order to install the application the network administrator can use the installation service using an SMS message (for details see Kaspersky Mobile Security 7.0 Enterprise Edition Administrator’s Guide). An SMS message containing the URL of the server on which the application installation kit is located will be sent to the mobile device.

In order to install the application using an SMS message, perform the following actions:

1. Open an SMS containing URL of the server from which the Kaspersky Mobile Security installation package will be downloaded.
2. Use the link contained in the message text to download the application installation kit onto the device.
3. Save the application installation kit.

1.4. Activating the application

Note

Activation of the application is required. Otherwise the application's functionality will not be available.

Activation of Kaspersky Mobile Security 7.0 Enterprise Edition is performed during synchronization with the Administration Server. During the synchronization the key file specified in the course of creating the policy for mobile devices (for more details about Kaspersky Administration Kit policies for mobile devices see Kaspersky Mobile Security 7.0 Enterprise Edition's Administrator's Guide) is copied to the device.

The process of the application synchronization with the Administration service will be started automatically with the interval specified in the policy for mobile devices. You can also start the synchronization process manually (see section 2.1.9 on page 30 or on section 3.6 on page 53).

Note

While the policy is being created the possibility of mobile device key file modification must be blocked. Otherwise the device will not be activated during the synchronization with the Administration Server.

CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS

This chapter contains description of the operation of Kaspersky Mobile Security 7.0 for devices running Symbian version 9.1, 9.2 or Series 60 UI operating system.

2.1. Using the application

This section contains information about configuration of the settings of the anti-virus scan and real-time protection, SMS message filtering, device anti-virus scan, bases update, application operation settings, device protection at the network level, etc.

2.1.1. Starting the application

In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the device's main menu.
2. Select **KMS 7.0 EE** and start the application using the **Open** item from the **Options** menu.

After the device startup a window with main Kaspersky Mobile Security components (see Figure 2) will be displayed on the device screen.

- **Real-Time Protection** - using the real-time protection mode (see section 2.1.4 on page 12);
- **Last Full Scan** – date of the last anti-virus device scan.
- **Database date –** release date of the anti-virus database used by the application.
- **Anti-Spam Config.** – Anti-Spam operation mode (see section 2.1.6 on page 19).
- **Firewall level** – device protection level at the network level (see section 2.1.9 on page 30).

Figure 2. The Application component status window

In order to switch to the application interface, press **OK**.

2.1.2. Graphical user interface

The graphical user interface (GUI) contains six tabs:

- Using the **Scan** tab you can perform an anti-virus can of the device, edit the anti-virus scan, real-time protection and quarantine settings and configure the auto scan schedule.
- Using the **Update** tab you can update the anti-virus database, edit the updating settings and configure the updating schedule.
- Using the **Firewall** tab you can monitor the network activities and protect device at the network level.
- The **Anti-Theft** tab allows blocking the device and erase information from it in case the device gets lost or stolen (Anti-Theft module).
- Using the **Anti-Spam** tab you can configure filtering of incoming SMS messages (Anti-Spam module).
- Using the **Information** tab you can view application component's operation logs, general information about the application and the anti-virus bases used and edit general settings used for application's operation.

To navigate from one tab to another, use the joystick of the device or select the **Open page** item in the **Options** menu (see Figure 3).

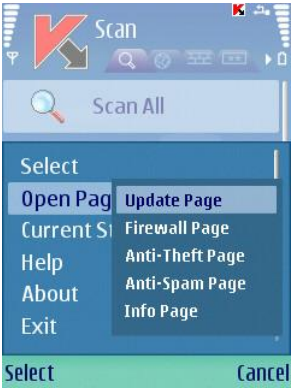

Figure 3. The **Options** menu

In order to return to the application components status window, select the **Current status** item in the **Options** menu.

2.1.3. General settings

Using settings in the **Information** tab in the **Settings** item (see Figure 4) you can configure the following application's functions:

- **Show status screen** determines whether the current status will be displayed at the application startup.
- **Log size** determines the maximum log size. Once the minimum value of the specified threshold has been reached, older messages in the log will be deleted until the maximum value of specified threshold is reached.
- **Screen backlighting** determines whether the screen will be lit during the anti-virus scan. By default the backlight option is disabled.
- **Play sound** controls the use of the sound notification in case of certain events (detection of an infected objects, message about an application status, etc.) By default the playback of the sound signal in case of a virus detection depends on the device profile (the setting's value **Profile dependent**). Select **Enabled** if you wish to use the sound notification irrespective of the device profile selected.
- **Sound volume** determines the volume of the sound notification playback in case of the detection of an infected object.

- **Vibration** determines whether the device will vibrate when an infected object is detected. By default vibration is enabled.

Figure 4. The **Settings** menu

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

2.1.4. Anti-virus scan and protection

Using the **Scan** tab you can perform anti-virus scan of the entire file system and the memory of the device or of an individual folder or file. You can also modify the settings of the anti-virus scan and of the real-time anti-virus protection, view the report about the scan results and create the automatic scan start schedule.

2.1.4.1. Real-time protection and on-demand scan

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the device's RAM and monitors all data including the incoming data received by the device.

Real-time protection is started since the moment the device is turned on and works until it is turned off (if the use of this mode was not disabled by the protection settings).

Kaspersky Mobile Security also allows to perform a full scan of the device's file system including the analysis of objects located on the connected memory expansion cards.

Information about the results of the real-time protection and of the on-demand scan will be recorded in the report. In order to view the report, select the **Reports** item in the **Scan** tab.

To start Real-Time protection, do the following:

1. Select the **Settings** item in the **Scan** tab.
2. Select the **Monitor settings** in the **Settings** section.
3. Enable / disable real-time protection by setting the **Real-Time Protection** setting certain value to a corresponding value.

To modify the Real-Time protection operation settings, do the following:

1. Select the **Settings** item in the **Scan** tab.
2. Select the **Monitor settings** in the **Settings** section.
3. Define the scan area in the **Scan mask** block by selecting the file types to be scanned:
   - **All files** – scan all files.
   - **Executable files** – scan only executable program files (for example *.exe, *.sis, *.mdl, *.app).
4. Determine the action to be performed when an infected object has been detected (the **Virus found action** setting).

   By default detected malware objects are placed into quarantine (the **Quarantine** setting value).

   To ensure that information about detection of an infected object is logged in the application's report, select value **Log event**.

   To make the application delete detected malware objects without prompting user for action, select the **Auto delete** value.
5. Enable / disable new card scan mode (the **Scan new card** setting).

   By default, if a memory card is detected, the application notifies that the card must be scanned.

   To enable the scan of flash-cards, connected to the device, set the **Auto scan** value. In order to disable the automatic scan of flash cards, select **Disable**.
6. Enable / disable the display of the protection icon (the **Show monitor icon** setting).

   Select the **Always** value in the corresponding item of the menu if you wish the application icon to be always displayed on the device's screen when the real-time protection is enabled. If you wish the icon to be dis-

played only in the device's menu, select **In menu only**. If you do not wish this icon to be displayed, select **Off**.

To modify the on-demand scan operation settings, do the following:

1. Select the **Settings** item in the **Scan** tab.
2. Select the **Scan settings** in the **Settings** section.
3. Define the scan area in the **Scan mask** block by selecting the file types to be scanned:
   - **All files** – scan all files.
   - **Executable files** – scan only executable program files (for example *.exe, *.sis, *.mdl, *.app).
4. Determine the action to be performed when an infected object has been detected (the **Virus found action** setting).

   By default the application attempts to disinfect detected malware objects (the setting value **Try to disinfect**).

   To place detected malware objects into quarantine, select the **Quarantine** value.

   To ensure that information about detection of an infected object is logged in the application's report, select value **Log event**.

   To make the application delete detected malware objects without prompting user for action, select the **Auto delete** value.

   To ensure that a notification with a prompt for action is opened once an infected object is detected, select the **Ask user** value.
5. Specify an action to be performed if disinfection of an infected object is impossible (**If disinfection fails** setting).

   By default detected malware objects are placed into quarantine (the **Quarantine** setting value).

   To ensure that information about detection of an infected object is logged in the application's report, select value **Log event**.

   To make the application delete detected malware objects without prompting user for action, select the **Auto delete** value.

   To ensure that a notification with a prompt for action is opened once an infected object is detected, select the **Ask user** value.
6. Enable / disable the scan of the device ROM memory (the **Scan ROM** setting).

In some situations the ROM memory may become vulnerable for malware programs. To enable ROM memory scan, select the **Yes** value.

7. Enable / disable unpacking of SIS and ZIP archives (the **Unpack archives** setting).

   If you wish the application unpack SIS and ZIP archives, select **Yes**. If archives do not need to be unpacked during the scan, select **No**.

Note

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

By default the application uses the values of the settings recommended by Kaspersky Lab's specialists. If you wish to return to the recommended values of the settings while you are using the application, open the **Scan** tab and select the **Set default** item from the **Options** menu.

In order to start an anti-virus scan, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Using the **Scan** tab (see Figure 5) select the **Scan all** item if you wish to scan the entire file system of the device or **Scan folder** if you wish to scan an individual folder.

Figure 5. The **Scan** tab

When **Scan folder** item is selected, a window displaying the device's file system will open. In order navigate through the file system use the joystick buttons of your device. In order to scan a folder, move the cursor to the folder you wish to scan and select the **Start scanning** item from the **Options** menu.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of scanned objects, the path to the object being scanned at the time and the percentage indicator of the progress (see Figure 6).

Figure 6. The **Scan progress** window

Once an infected object is detected the action specified by the corresponding setting in the **Settings→Scan settings** section will be performed.

Figure 7. Notification about virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

To disable screen backlight during the scan,

switch to the **Information** tab, open the **Settings** menu and select the **Yes** value for the **Screen backlighting** setting.

By default the backlight will go off automatically to save the battery charge.

2.1.4.2. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic device scan. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (see section 2.1.4.1 on page 12).

By default scheduled scan is disabled.

Figure 8. The **Schedule** menu

To create the scan launch schedule:

select the **Schedule** item in in the **Scan** tab and specify the **Auto scan** settings (see Figure 8):

- **Daily** - the scan to be performed every day. Specify the **Auto scan time** in the entry field.
- **Weekly** - the scan will be performed once a week. Specify the **Auto scan day** and **Auto scan time**.

2.1.5. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for the device and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

If you wish the application to place detected malware objects into the quarantine without the prompt, do the following:

1. Open the **Scan** tab.
2. Select the **Settings** item.
3. Select the **Scan settings** or the **Monitor settings** item.
4. Select **Quarantine** as the value for the **Virus foud action** setting.

If you selected **Ask user** as the action to be performed, then, when an infected object is detected, Kaspersky Mobile Security will offer that you either delete this object or quarantine it.

To view the list of quarantined objects,

open the **Scan** tab and select the **Quarantine** item (see Figure 9).

Figure 9. Infected quarantined objects

The **Options** menu accessible from the quarantine view window allows the user:

- To view detailed information about each object in the quarantine (**View details**).
- Delete the selected object (**Remove file**).
- Clear the quarantine by deleting all quarantined objects (**Remove all**).
- Restore the selected object from the Quarantine to its original folder (**Restore file**).
- **V**iew Quarantine Help (**Help**).

In order to set the quarantine settings:

1. Open the **Scan** tab.

2. Select the **Settings** item.
3. Select the **Quarantine** tab (see Figure 10).

Figure 10. Quarantine settings

The **Quarantine size** setting determines the maximum number of infected objects which can be stored in the quarantined. The possible values are **20**, **50** or **100** files.

The **Store limit** setting determines the period of time during which the infected objects can be stored in the quarantine. After this period elapses, the infected objects will be automatically deleted.

Note

In order to restore the values of the quarantine settings recommended by Kaspersky Lab's specialists select **Set default** from the **Options** menu.

2.1.6. Using Anti-Spam

The Anti-Spam module is designed to ensure protection of your device against unsolicited SMS messages.

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender's number is included into the "black" list;
- check if the sender's number is included into the "white" list;

- scan of the message text for the presence of phrases found in the “black” list;
- scan of the message text for the presence of phrases found in the “white” list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the “black” list will be blocked. The message containing an element found in the “white” list will be passed.

2.1.6.1. Anti-Spam work modes

Anti-Spam filters messages in one of the following modes:

- **Enabled.** In this mode Anti-Spam filters incoming messages using the "black" and the "white" lists. Once a message is received from a phone number not found in either of the lists, Anti-Spam will notify the user and will offer to block or allow receipt of the message and to add this phone number to the "white" or "black" list.
- **Black List.** In this mode Anti-Spam blocks receipt of messages matching the “black list” criteria. All other messages will be passed.
- **White List.** In this mode Anti-Spam passes messages matching the “white list” criteria. All other messages will be blocked.
- **Disabled.** In this mode Anti-Spam is disabled. No filtering of incoming messages is provided.

To select the Anti-Spam operation mode:

1. Open the **Anti-Spam** tab.
2. Select the **Settings** item.
3. Set the operation mode using the **Anti-Spam config.** setting.

2.1.6.2. Editing “black” and “white” lists

"Black" and **"White"** lists contain records with phone numbers, SMS from which will be block or passed by Anti-Spam. Information about blocked or deleted messages will be entered in the **Log** section.

Note

Messages not included into either list will not blocked!

To enter changes into the "black" or "white" list,

open the **Anti-Spam** tab and select the corresponding item (see Figure 11).

To edit the list use the **Options** menu:

- **Add number** – add a new record to the list.
- **Edit number** – edit the current record.
- **Remove number** – delete entry from the list.
- **Remove all** – clear the list by deleting all records.
- **Help** – view Help on managing the list.

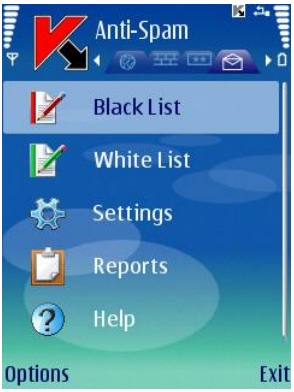

Figure 11. The **Anti-Spam** tab

When you select the **Add number** or the **Edit number** item, you will be offered to specify the following record's parameters (see Figure 12)

- **Number**. Specify the phone number for which receipt of messages will be blocked or allowed. Such number may begin with a digit or with a "+" and must contain digits only. Additionally when specifying a number, you can use masks "?" and "*".
- **Text**. Specify the text upon detection of which in the message received, such message will either be passed or blocked.

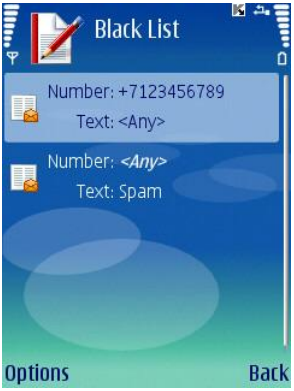

Figure 12. The Black List

2.1.6.3. Anti-Spam operation settings

To edit Anti-Spam settings:

open the **Anti-Spam** tab and select the **Settings** item (see Figure 13).

Figure 13. Anti-Spam settings

The following Anti-Spam settings are accessible in the **Settings** menu:

- **Anti-Spam config.** – Anti-Spam operation mode (see section 2.1.6.1 on page 20).
- **Allow contacts list**. If the setting is assigned value **Yes**, Anti-Spam will not block receipt of messages from numbers contained in your phone book. If this option is disabled (**No** value), Anti-Spam will perform filter-

ing depending on whether the phone number is included into the "white" or "black" list.

- **Add outgoing**. If the setting is assigned value **Yes**, all phone numbers to which you send SMS messages will be automatically added to the "white" list. To disable this option, select **No**.
- **Block non-numeric.** If this setting is assigned value **No**, Anti-Spam will not block all incoming messages from non-numeric numbers. To enable this option, select **Yes**.

> **Note**
>
> This setting affect only records created by Anti-Spam in one of the following situations:
>
> - adding outgoing numbers to the "white" list (setting **Add outgoing** is enabled);
> - adding new phone numbers from which messages are received to one of the lists (see section 2.1.6.4 on page 23).

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

2.1.6.4. Actions to be performed with messages

When you receive an SMS or an MMS message from a phone number not found in either the "black" or the "white" list, such message will be intercepted by Anti-Spam and a notification will be displayed on the screen of the device (see Figure 14)

Using the **Options** menu you can select one of the following actions to be performed with the message:

- **Add to White List** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to Black List** – block messages and add the sender's phone number to the "black" list.
- **Skip** – allow the receipt of the message. In this case the sender's phone number will not be added to either of the lists.

Information about blocked messages will be entered into the application log. In order to view the report, select the **Reports** item in the **Anti-Spam** tab.

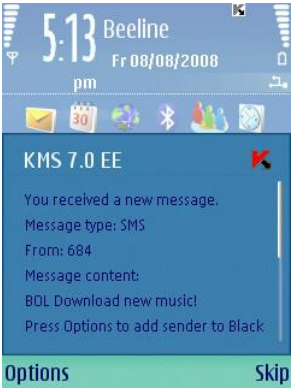

Figure 14. Anti-Spam warning

2.1.7. Using Anti-Thief

The Anti-Thief module is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was list or stolen.

When you access the module settings for the first time you will have to set up a password. Later this password is used to obtain access to the module's settings and managing its functions. **SMS-Block** function – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. To unblock the device using the SMS-Block function, send an SMS message containing text: `"block:code"` to the device. By default the SMS-Block function is disabled. To enable the function select **On**.

The **SMS-Clean** allows erasing user's personal data (contacts, messages, files, data from the memory card, network settings). To use the SMS-Clean function, send an SMS containing text "clean:code" to the device. By default the SMS-Clean function is disabled. To enable the function select **On**.

SIM Watch – allows to send to the specified numbers a new phone number and to block the stolen device if the SIM card was replaced in such stolen device. To enable the function select **On**.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change code** item. Enter the new password and its confirmation and press the **OK** button.

Each time when you access the Anti-Theft module settings (see Figure 14) you have to enter the password you have set up earlier.

Figure 15. The **Anti-Theft** tab

Information about the module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Anti-Theft** tab.

2.1.7.1. Section SMS-Clean

To configure the SMS-Clean function operation settings:

1. Open the **Anti-Theft** tab and enter the password (see section 2.1.7 on page 24).
2. Select the **Settings** item.
3. Select the **SMS-Clean** item.

Section **SMS-Clean** contains the list of data which can be selected for deletion if your device gets lost (see Figure 16).

Figure 16. The **SMS-Clean** tab

If you wish to be able to delete the phone book once your mobile device has been stolen or lost, select the **Remove contacts** item and assign value **Yes** to it.

Note

Contacts will be erased only from the phone book stored in the device. SIM card phone book will not be deleted.

In order to delete mail, SMS messages (Inbox and Mailbox folders) select the **Clean inbox** and assign value **Yes** to it.

The **Delete personal files** item ensures deletion of personal data (data from folder !:\Data\). By default deletion of personal files is not provided. If you wish to be able to delete your personal data in case your device is stolen or lost, select this item and assign value **Yes** to it.

Use the **Delete card files** item to enable clearing the memory card on the lost device. By default this ability is disabled. To enable erasing of data from the memory card, select the **Delete card files** and select the **Yes** value.

To enable the option of deleting network connection settings, select the **Delete network settings** item and set the value to **Yes**.

Press **OK** to save the changes.

2.1.7.2. SIM Watch settings

To configure the SIM Watch settings, switch to the **Anti-Theft** tab. Enter the password (see section 0 on page 24) and then select **SIM Watch** in the window that will open.

Section **SIM Watch** is designed to monitor replacement of the SIM card in the device (see Figure 17).

Figure 17. The **SIM Watch** tab

Using fields **Phone number 1** and **Phone number 2** enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your device. Such numbers may begin with a digit or with a "+" and must contain digits only.

Also you can enable blocking your device if the SIM card was replaced. To do it, select the **Block device** item and assign value **Yes** to it. You can unblock the device by entering the password set up to access the Anti-Theft module. By default blocking of the device is not provided.

Press the **OK** button to save the changes you have made.

2.1.8. Updating the application bases

Scan for malware programs is performed based on the records in the application's bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. Updates are performed from Kaspersky Lab's servers via internet.

You can enable automatic anti-virus scan of your device after each update of the Kaspersky Mobile Security bases. In order to do it, switch to **Settings** item in the **Update** tab and assign value **On** to the **Scan on update** item.

The value of the **Scan Quar. on update** setting determines whether or not objects in the quarantine will be rescanned each time after the application bases

have been updated. By default the scan is performed. If you do not wish the scan to be performed, select **Off**.

If it is necessary to change the active access point, use the **Access point** setting. Then select the require value in the list. By default the access point is the default point of the device.

The value of the **Update server** setting determines the application bases update source: Kaspersky Lab's update servers (**Use default** value) or another server specified by the user (**User defined** value). If you selected the **User defined** value, enter the URL in the window that will open. If required, you can specify an alternative update server.

You can view detailed information about bases used in the **Database info** item in the **Information** tab.

Information about bases update will be entered into the log. In order to view the log, select the **Reports** item in the **Update** tab.

2.1.8.1. Updating settings

In order to configure application bases updates, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Switch to the **Settings** item in the **Update** tab (see Figure 18).

Figure 18. The **Updater** Tab

3. Select the access point (the **Access point** setting) (see Figure 19).

Note

The access point is configured using settings provided by your wireless service provider.

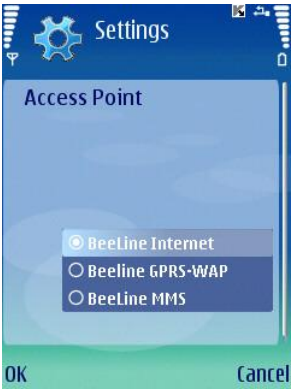

Figure 19. Selecting the access point

4. Enter the address of the update server (if necessary). In order to do it, select the **Update server** item and then select the **User defined** value. Enter the URL of the update source in the window that will open (see Figure 20).

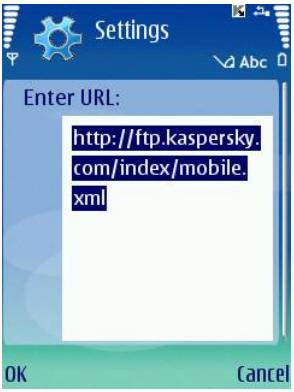

Figure 20. Update server address

By default updates are performed from Kaspersky Lab's update server: http://ftp.kaspersky.com/index/mobile.xml.

Note!

Irrespective of whether the connection was opened earlier, it will be closed after the update is complete.

2.1.8.2. Manual update

To start a manual update of Anti-Virus databases:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Select the **Update** item in the **Update** tab (see Figure 18)

2.1.8.3. Scheduled update

To create an application bases update launch schedule.

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Select the **Schedule** item in the **Update** tab and configure the **Auto update** settings:
   - **Off** – to not perform scheduled updates.
   - **Daily** - the update to be performed every day. Specify the update time in the corresponding field.
   - **Weekly** - the update will be performed once a week. Specify the update date and time in the corresponding fields.

2.1.9. Updating the application operation settings

Note

For details about the joint operation of Kaspersky Mobile Security and Kaspersky Administration Kit see Kaspersky Mobile Security Administrator's Guide.

While using Kaspersky Mobile Security jointly with Kaspersky Administration Kit the application operation settings will be set by the policy for a group of mobile devices. Activation of the application and the applying of the policy settings blocked to prevent changes will take place when a device is being added to the administration group.

Later synchronization of the application with the Administration Server will be performed automatically using intervals set in the policy settings.

In order to start application manual synchronization with the Administration Server:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Open the **Update** tab.
3. Select **Synchronization** item.

During the synchronization the application operation settings will be loaded from the Administration Server and reports about the application's operation will be sent from the device to the application server. If the application operation settings did not change since the time of the last synchronization, the policy settings will not be applied.

2.1.10. Using the Firewall module

Firewall module is designed for monitoring the network activity and protection of your mobile device at the network level (see Figure 21).

You can select the protection level (**Firewall** setting) in order to specify the level of control over the incoming and outgoing traffic out of the suggested options:

- **High** – any network activity except updating of bases and connection to Kaspersky Administration Kit is blocked.
- **Medium** – all incoming connections will be blocked, outgoing connections can only be established using SSH, HTTP, HTTPS, IMAP, SMTP, POP3 ports.
- **Low** – only incoming connections will be blocked.
- **Off** – all network activities will be allowed.

Using the **Notifications** setting you can enable/disable the user's notification about an attempt to establish a connection blocked at the Firewall protection level selected. In order to disable receipt of notifications, select **Off**.

Figure 21. The **Firewall** tab

Information about the Firewall module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Firewall** tab.

2.1.11. Viewing report about the application operation

You can view the chronological event log about the operation of Kaspersky Mobile Security in the **Information** tab. In order to do it switch to this tab and select the **Reports** item (see Figure 22).

Figure 22. Report about the application's work

2.2. Uninstalling the application

In order to uninstall Kaspersky Mobile Security, perform the following actions:

1. Close Kaspersky Mobile Security. To do this:
   a) Press and hold the **Menu** button.
   b) Select **KMS 7.0 EE** in the list of the running applications and press the **Options** button.
   c) Select the **Close** menu item (see Figure 23).

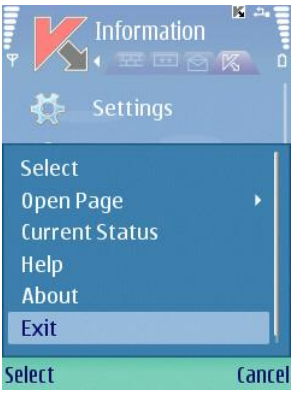

Figure 23. Closing the application

2. Uninstall Kaspersky Mobile Security
   a) Press the **Menu** button and select the **Application manager** menu item (see Figure 24).

Figure 24. Starting the **Application Manager**

b) Select **KMS7.0 EE** in the list of applications and press the **Options** button (see Figure 25).

Figure 25. Selecting the application

c) Select the **Remove** menu item (see Figure 26).

Figure 26. Uninstalling the application

d) Press the **Yes** button in the prompt to confirm the application removal.

CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE

This chapter contains description of the operation of Kaspersky Mobile Security for mobile devices running one of the following operating systems:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

3.1. Getting started

This section contains information on how to start the application. It also contains information about the general principles of the graphic user's interface.

3.1.1. Starting the application

In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the **Programs** menu on your mobile device.
2. Select **KMS 7.0 EE** in order to start the application.

After the application startup a window with main Kaspersky Mobile Security components (see Figure 27) will be displayed on your mobile device's screen.

- **Real-Time Protection** – the use of the real-time protection mode.
- **Last scanned** – date of the last anti-virus scan of your mobile device.
- **Last updated –** release date of Kaspersky Mobile Security database used by the application.

> **Note!**
>
> If anti-virus scan of your mobile device has never been performed or if it two weeks or more have passed since the last update of the anti-virus database, the icon next to the corresponding item will look as follows: ⚠. This icon will also appear if the real-time protection mode or the Anti-Spam modules is disabled.

- **Firewall** – device protection level at the network level.
- **Anti-Spam** – the status of the Anti-Spam module used for filtering SMS messages.

> **Note!**
>
> Anti-Spam module is not provided for PDAs!

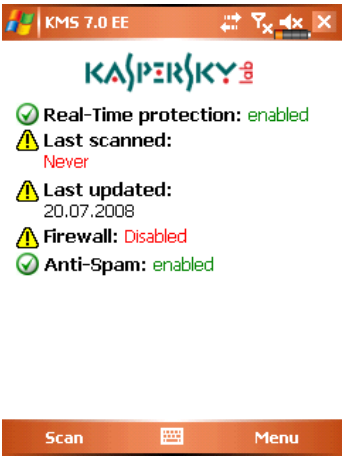

Figure 27. The application component status window

3.1.2. Graphical user interface

The graphical user's interface consists of six tabs access to which is provided via **Menu** (see Figure 28):

- Using the **Scan** section you can perform an anti-virus can of the mobile device, edit the anti-virus scan, real-time protection and quarantine settings and create the auto scan schedule (see section 3.2 on page 38).
- Using the **Firewall** section you can monitor the network activities and protect the device at the network level (see section 3.7 on page 53).

- Using the **Update** section you can update the anti-virus database, edit the updating settings and configure the updating schedule (see section 3.5 on page 51).
- Using the **Anti-Spam** section you can configure filtering of incoming SMS messages (Anti-Spam module) (see section 3.4.1 on page 45).
- Using the **Anti-Theft** section you can block the device and erase information stored on it in case it gets lost or stolen (the Anti-Theft module) (see section 3.4.2 on page 48).
- Using the **Information** section you can view application components' operation logs, general information about the application and bases being used (see section 3.8 on page 54).

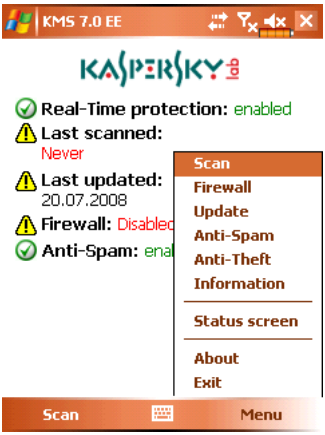

Figure 28. The application menu

In order to return to the application components status window, select the **Status screen** item.

To view the general information about the application, select the **About** item.

To close the application, select **Exit**.

3.2. Anti-virus scan and Real-Time protection

Using the **Scan** section you can perform anti-virus scan of the entire file system and the memory of the mobile device or of an individual folder or file. You can also modify the settings of the anti-virus scan and of the real-time anti-virus pro-

tection, view the report about the scan results and create the automatic scan start schedule.

3.2.1. On-demand scan

To modify the on-demand scan settings, do the following:

1. Select the **Scan settings** in the **Scan** section.
2. Define the scan area in the **Scan options** block by selecting the file types to be scanned:
   - **Scan archives** - scan files packed into archives.
   - **Executables only** - scan only executable program files.
3. In the **If a virus is detected** block, determine the action to be performed by the application once an infected object is found. If disinfection is not required, select the possible anti-virus action by selecting one of the following values for the **Primary action** setting:
   - **Quarantine** – move infected objects detected to the quarantine.
   - **Ask user** - display a message about a virus detection on the screen with a suggestion to delete, quarantine or skip the infected object.
   - **Delete** - delete infected objects detected.
   - **Skip** – do not perform any action with the infected objects.

   If you want the application to attempt to disinfect a detected infected object, check the **Try to disinfect** box. Select an action to be performed by the application if disinfection is impossible in section **If disinfection fails**.

In order to start an anti-virus scan, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 36).
2. Using the **Scan** section (see Figure 29) select the **Scan phone** item if you wish to scan the entire file system of the mobile device or **Scan folder** if you wish to scan an individual folder.

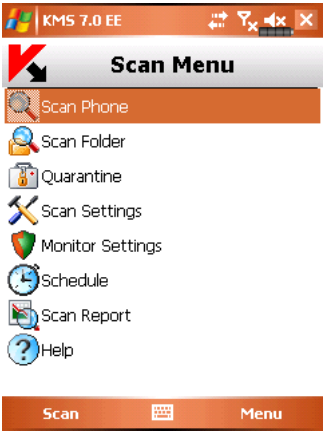

Figure 29. The **Scan** section

When **Scan folder** item is selected, a window displaying the mobile device's file system will open. In order to start the scan of a folder, move the cursor to the folder and press the **Scan** button.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of objects scanned and the path to the object currently being scanned (see Figure 30).

Figure 30. The **Scan progress** window

Figure 31. Notification about virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

3.2.2. Real-time protection

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the mobile device's RAM and scans executable program files and files being opened by the user.

Real-time protection is started since the moment the device is turned on and works until it is turned off (if the use of this mode was not disabled during configuration of the protection settings).

Additionally, Kaspersky Mobile Security allows to perform a full scan of the mobile device's file system.

Information about the results of the Real-time protection and of the on-demand scan will be recorded in the report. To view the report, select the **Scan report** item. The report is also available in the **Information** section (see section 3.8 on page 54);

To enable Real-Time protection, do the following:

1. Select the **Monitor settings** in the **Scan** section.
2. Check the **Enable Real-Time Prot.** box.

To modify the Real-Time protection operation settings, do the following:

1. Select the **Monitor settings** in the **Scan** section.
2. Check the **Executables only** box in the **Scan options** section if you wish Real-Time protection to scan only executable program files. Uncheck the box to make Real-Time Protection to scan executable program files and files being opened by the user.
3. In the **If a virus is detected** block, select the action to be performed by the application once an infected object is found. You can select one of the following options:
   - **Quarantine** – move infected objects detected to the quarantine.
   - **Delete** - delete infected objects detected.
   - **Skip** – do not perform any action with the infected objects.

3.2.3. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic scan of the mobile device. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (the **Scansettings** item).

By default scheduled scan is disabled.

In order to create a schedule for launching a device's file system scan:

select the **Schedule** item in the **Scan** section and create a scan launch schedule (see Figure 32):

- **Daily** - the scan to be performed every day. The scan time is determined by the **Time** setting.
- **Weekly** - the scan will be performed once a week. The date and time of the scan will be determined by settings **Weekday** and **Time**.
- **Manually** - the update will be manually launched by the user.

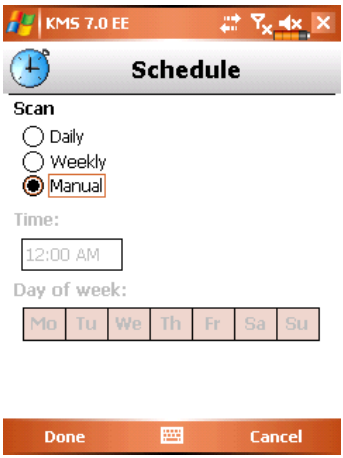

Figure 32. The **Schedule** menu

3.3. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for the mobile device and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

In order to enable automatic movement of infected objects to the quarantine:

1. Open the **Scan** section,
2. Select the **Scan settings** item.
3. In the **If a virus is detected** section select **Quarantine** as the action to be performed in case of a detection of a malware object.

   If you select **Ask user** as the action to be performed, then, once an infected object is detected, a notification window containing a prompt to either delete the object or quarantine it.

In order to view quarantine content,

open the **Scan** section and select the **Quarantine** item (see Figure 33).

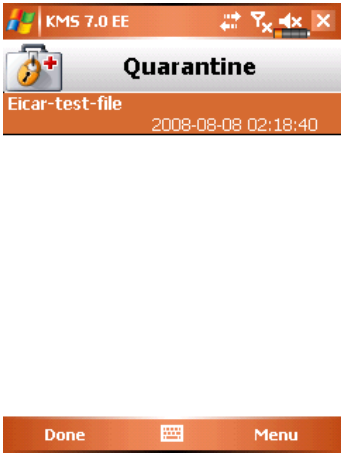

Figure 33. **Quarantine**

The **Menu** accessible from the quarantine view window allows the user:

- To view detailed information about the selected object in the quarantine (**Detailed info** item).
- Delete the selected object (**Delete file** item).
- Restore the current object from the Quarantine to its original folder (**Restore** item).
- Clear the quarantine by deleting all quarantined objects (**Empty quarantine** item).

3.4. Using Anti-Spam and Anti-Theft modules

The Anti-Spam module is designed to ensure protection of your device against unsolicited SMS messages.

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender's number is included into the "black" list;
- check if the sender's number is included into the "white" list;

- scan of the message text for the presence of phrases found in the “black” list;
- scan of the message text for the presence of phrases found in the “white” list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the “black” list will be blocked. The message containing an element found in the “white” list will be passed.

3.4.1. Anti-Spam module

The Anti-Spam module is designed to ensure protection of your device against unsolicited SMS messages.

Note!

Anti-Spam module is not provided for PDAs!

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender’s number is included into the "black" list;
- check if the sender’s number is included into the "white" list;
- scan of the message text for the presence of phrases found in the “black” list;
- scan of the message text for the presence of phrases found in the “black” list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the “black” list will be blocked. The message containing an element found in the “white” list will be passed.

To edit Anti-Spam settings do the following:

1. Select **Settings** in the **Anti-Spam** section.
2. Select the operation mode using the **Anti-Spam** using the **Anti-Spam** setting:
    - **Normal.** In this mode Anti-Spam filters incoming messages using the "black" and the "white" lists. Once a message is received from a phone number not found in either of the lists, Anti-Spam will notify the user and will offer to block or allow receipt of the message and to add this phone number to the "white" or "black" list.

- **“Black” list only.** In this mode Anti-Spam blocks receipt of messages matching the “black list” criteria. All other messages will be passed.
- **“White” list only.** In this mode Anti-Spam passes messages matching the “white list” criteria. All other messages will be blocked.
- **Disabled.** In this mode Anti-Spam is disabled. No filtering of incoming messages is provided.

3. Check the **Allow contacts** box so that Anti-Spam would not block receipt of messages from numbers found in the contact list.
4. Check the **Block non-numeric** box so that Anti-Spam would block receipt of messages from non-numeric numbers.

3.4.1.1. Editing “black” and “white” lists

The “Black” list contains entries which, if found in messages, makes Anti-Spam block such messages.

The “Black” list contains entries, which, if found in messages, makes Anti-Spam block such messages.

To edit the "black" or "white" list,

open the **Anti-Spam** section (see Figure 34) and select the corresponding list.

To edit the list use the **Menu**:

- **Add number** – add a new record to the list.
- **Remove number** – delete record from the list.
- **Edit number** – edit the current record in the list.

Select the **Add number** item and specify your phone number (field **Enter phone**) you wish to be included into the list. This number may begin with a digit or with a "+". Additionally when specifying a number, you can use masks "?" and "*".

You can also specify the text (**Enter text** field) upon the detection of which in a message the following actions will be performed:

- the message in which such text specified for the "white" list is found will be allowed to pass;
- the message in which such text specified for the "black" list is found will be blocked;

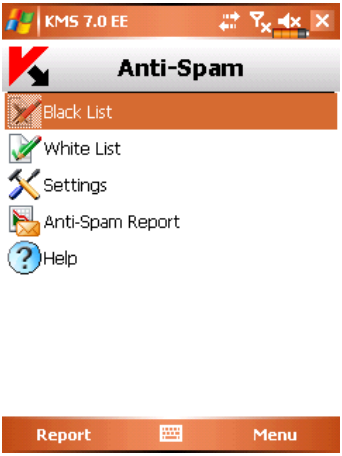

Figure 34. The **Anti-Spam** section

After you are done editing the list, press **Done** to return to the **Anti-Spam** section.

3.4.1.2. Actions to be performed with messages

When you receive messages from a phone number not found in the "black" or "white" list depending that the Anti-Spam settings allow the receipt of message from unknown numbers (see section 3.4.1 on page 45), a warning will be displayed on the mobile device's screen (see Figure 35).

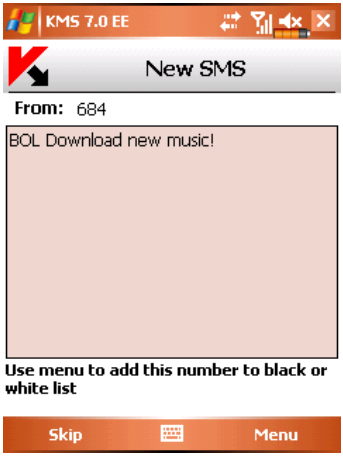

Figure 35. Anti-Spam warning

Using the **Menu** you can select one of the following actions to be performed with the message:

- **Add to WhiteList** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to BlackList** – block messages and add the sender's phone number to the "black" list.

Press the **Skip** button in order to let the message pass. In this case the sender's phone number will not be added to either of the lists.

Information about blocked messages will be entered into the application log.

In order to view the log, select the **Anti-Spam report** item in the **Anti-Spam** section. The report is also available in the **Information** section (see section 3.8 on page 54);

3.4.2. The Anti-Theft tab

The Anti-Thief module (section **Anti-Theft** (see Figure 36) is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was list or stolen.

When you access the module settings for the first time you will have to set up a password. Using this password you can obtain access to the module's settings and activate the module functions. The password is required in order to prevent

unauthorized access to the module operation settings and to enable the user to block and erase information saved on the device in case it is stolen or lost.

SMS-Block function – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. The action of this function gets triggered after the user sends an SMS message “block:code” to the device that got lost.

SMS-Clean allows erasing user's personal information (contact, incoming messages, personal files, network connection settings). The action of this function gets triggered after the user sends an SMS message “clean:code” to the device that got lost.

The **SIM Watch** allows sending a new phone number to the specified numbers in case the device is lost and then – block this device. You can unblock the device by entering the password set up to access the Anti-Theft module.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change code** item. Enter the new password and its confirmation and press the **OK** button.

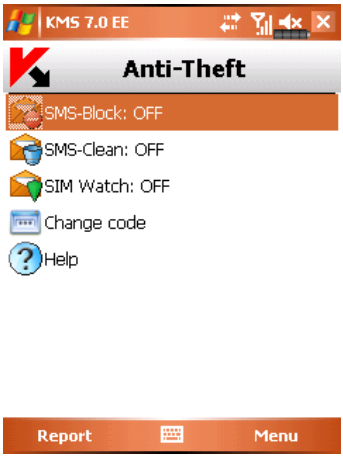

Figure 36. The **Anti-Theft** section

Information about the Anti-Theft module's work will be entered into the application log. To view the log, select the **Report** item in the **Anti-Theft** section. The report is also available in the **Information** section (see section 3.8 on page 54);

3.4.2.1. SMS-Clean function's settings

The **SMS-Clean** function allows erasing date from the device if it gets lost (see Figure 37).

In order to change the SMS-Clean function settings, perform the following:

1. Open the **Anti-Theft** section
2. Enter the password and select **SMS-Clean** in the window that will open.
3. Check the **contacts** box if you wish the phone book to be deleted once your mobile device has been stolen or lost.
4. Check the **inbox** box if you wish to erase mail and SMS messages.
5. Check the **documents** box if you wish to erase user's personal files.
6. Check the **network settings** box if you wish to erase the network connection settings.
7. Check the **files on the card** box if you wish to erase the files from the device memory card.
8. Press **Done** to save the changes.

Figure 37. SMS-Clean settings

3.4.2.2. SIM Watch function's settings

The **SIM Watch** function is designed to monitor replacement of the SIM card in the device (see Figure 38).

In order to change the SMS-Watch function settings, perform the following:

1. Open the **Anti-Theft** section
2. Enter the password and select **SIM Watch** in the window that will open.
3. Using fields **1)** and **2)** enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your device. Such numbers may begin with a digit or with a "+" and must contain digits only.
4. Check the **Block** box to enable blocking of the device if its SIM card has been replaced.
5. Press **Done** to save the changes you have entered.

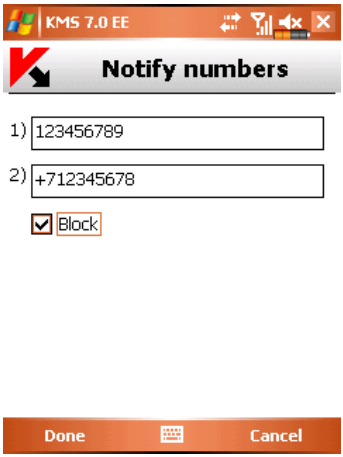

Figure 38. **SIM Watch** settings

3.5. Updating the application bases

Scan for malware programs is performed based on the records in the Kaspersky Mobile Security bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. To configure and start the update use the **Update** section (see Figure 39). Updates are performed from Kaspersky Lab's servers via internet.

Information about bases update will be entered into the log. In order to view the log select **Update report** in the **Update** section. The report is also available in the **Information** section (see section 3.8 on page 54);

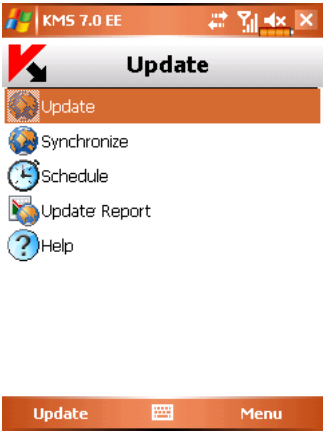

Figure 39. The **Update** section

In order to launch application bases updates manually, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 36) and open the **Update** section.
2. Select **Update** in order to start downloading updates.

To create an application bases update launch schedule, do the following.

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 36) and open the **Update** section.
2. Select the **Schedule** item.
3. Specify the update frequency in the **Automatic update** section:
   - **Daily** - the update to be launched every day. Additionally specify the **Time** of the update.
   - **Weekly** - the update will be launched once a week. Additionally specify the **Weekday** and the **Time** of the update.
   - **Manually** - the update will be manually launched by the user.

You can check the application base release date and the number of virus signatures it contains in the **Information** section. To do it, select the **About bases** item in this tab.

3.6. Updating the application operation settings

Note

For details about the joint operation of Kaspersky Mobile Security and Kaspersky Administration Kit see Kaspersky Mobile Security Administrator's Guide.

While using Kaspersky Mobile Security jointly with Kaspersky Administration Kit the application operation settings will be set by the policy for a group of mobile devices. Activation of the application and the applying of the policy settings blocked to prevent changes will take place when a device is being added to the administration group.

Later synchronization of the application with the Administration Server will be performed automatically using intervals set in the policy settings.

In order to start application manual synchronization with the Administration Server:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Open the **Update** section.
3. Select the **Synchronize** item.

During the synchronization the application operation settings will be loaded from the Administration Server and reports about the application's operation will be sent from the device to the application server. If the application operation settings did not change since the time of the last synchronization, the policy settings will not be applied.

3.7. Firewall

The **Firewall** module is designed for monitoring the network activity and protection of your mobile device at the network level (see Figure 40).

In order to change the Firewall settings, perform the following:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 36) and open the **Firewall** section.
2. Select the **Firewall settings** item. In the window that will open set the protection level to specify the level of monitoring of the incoming and outgoing traffic. You have the following options:

- **Block all** – any network activity except updating of bases and connection to Kaspersky Administration Kit is blocked.
- **Medium** – all incoming connections will be blocked, outgoing connections can only be established using SSH, HTTP, HTTPS, IMAP, SMTP ports.
- **Low** – only incoming connections are blocked.
- **Disabled** – all network activities are allowed.

Information about the operation of the Firewall will be entered into the log. In order to view the log, select **Update Report** in the **Update** section.

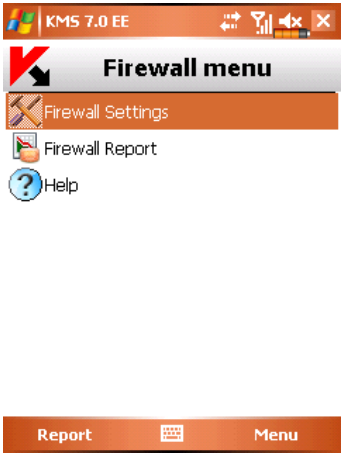

Figure 40. The **Firewall** section

3.8. Viewing reports about the application operation

Reports about the application's work are located in the **Reports** item of the **Information** tab. You can view a report on any task performed by Kaspersky Mobile Security:

- anti-virus scan;
- updating the application bases;
- firewall work;
- Anti-Spam module work;

- The Anti-Theft module work.

In order to view the report about the operation of one of the application components, do the following:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 36).
2. Select the **Reports** item in the **Information** section (see Figure 41).
3. Select the report of the required component in the window that will open.

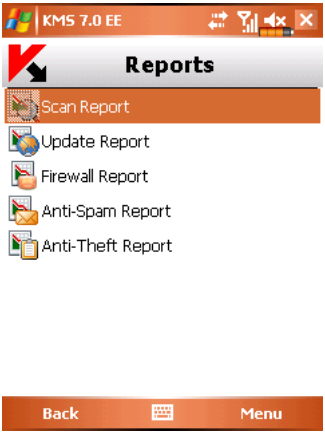

Figure 41. The **Reports** section

3.9. Uninstalling the application

In order to uninstall Kaspersky Mobile Security, perform the following actions:

1. Disable Real-Time Protection (for details see section 3.2 on page 38);

Figure 42. Disabling Real-Time protection

2. Close Kaspersky Mobile Security. To do it, select the **Exit** menu item (see Figure 43).

Figure 43. Closing the application

3. Uninstall the application. To do this:

   a) press the **Start** button, select the **Settings** menu, open the **System** tab and then switch to **Remove Programs** (see Figure 44):

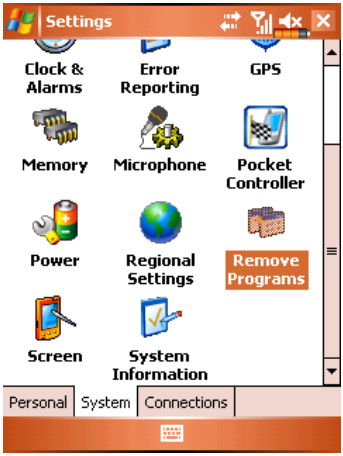

Figure 44. Starting removal of the application

b) Select **Kaspersky Mobile Security** in the list of installed applications and press the **Remove** button (see Figure 45).

Figure 45. Selecting the application

c) Press the **Yes** button in the application removal confirmation window (see Figure 46). After this a notification about removal of file containing the application operation settings will open. Press **No** button in order to uninstall the entire application. If you press the **Yes** button, the file with the application operation settings will be preserved on the device.

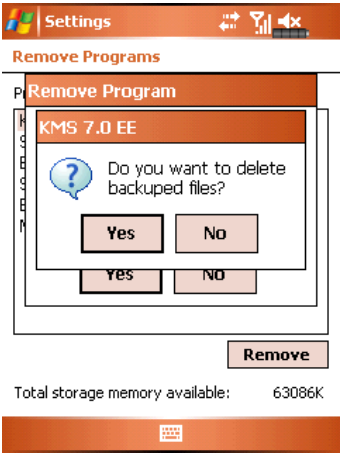

Figure 46. Prompt to save the application operation settings

APPENDIX A. KASPERSKY LAB

Kaspersky Lab was founded in 1997. Today it is the leading Russian developer of a wide range of high-performance information security software products, including anti-virus, anti-spam and anti-hacking systems.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has offices in the United Kingdom, France, Germany, Japan, the Benelux countries, China, Poland, Romania and the USA (California). A new company office, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network includes over 500 companies worldwide.

Today, Kaspersky Lab employs over a thousand highly qualified specialists, including 10 MBA degree holders and 16 PhD degree holders. All Kaspersky Lab's senior anti-virus experts are members of the Computer Anti-Virus Researchers Organization (CARO).

Our company's most valuable assets are the unique knowledge and collective expertise accumulated during fourteen years of continuous battle against computer viruses. Thorough analysis of computer virus activities enables the company's specialists to anticipate trends in the development of malware, and to provide our users with timely protection against new types of attacks. This advantage is the basis of Kaspersky Lab's products and services. The company's products remain one step ahead of other vendors in delivering comprehensive anti-virus coverage to our clients.

Years of hard work have made the company one of the top anti-virus software developers. Kaspersky Lab was the first to develop many of the modern standards for anti-virus software. The company's flagship product, Kaspersky Anti-Virus®, reliably protects all types of computer systems against virus attacks, including workstations, file servers, mail systems, firewalls, Internet gateways and hand-held computers. Its easy-to-use management tools maximize the automation of anti-virus protection for computers and corporate networks. A large number of developers worldwide use the Kaspersky Anti-Virus kernel in their products, including Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India), and BorderWare (Canada).

Kaspersky Lab's customers enjoy a wide range of additional services that ensure both stable operation of the company's products, and full compliance with the customer's specific business requirements. We design, implement and support corporate anti-virus systems. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with 24-hour technical support service in several languages.

If you have any questions, comments, or suggestions, you can contact us through our dealers, or at Kaspersky Lab directly. We will be glad to assist you,

via phone or email, in any matters related to our products. You will receive full and comprehensive answers to all your questions.

Kaspersky Lab official site:	http://www.kaspersky.com/
Virus Encyclopedia:	http://www.viruslist.com/
Anti-virus laboratory:	newvirus@kaspersky.com (only for sending archives of suspicious objects) http://support.kaspersky.ru/virlab/helpdesk.html (for queries to virus analysts)

APPENDIX B. CRYPTOEX LLC

To create and verify digital signatures, Kaspersky Anti-Virus uses Crypto Ex LLC's data security software library, Crypto C. CryptoEx LLC holds a license from the Federal Agency for Government Communications and Information (a branch of the Federal Security Service) and the Crypto C data security software library certificate.

CryptoEx LLC corporate website: http://www.cryptoex.ru

Exclusive rights for data security software library are reserved by CryptoEx LLC.

APPENDIX C. KASPERSKY LAB END USER LICENSE AGREEMENT

IMPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT BEFORE YOU START USING THE SOFTWARE.

BY CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR BY ENTERING CORRESPONDING SYMBOL(-S) YOU CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. **SUCH ACTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.** IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, CANCEL THE INSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE.

AFTER CLICKING THE ACCEPT BUTTON IN THE LICENSE AGREEMENT WINDOW OR AFTER ENTERING CORRESPONDING SYMBOL(-S) YOU HAVE THE RIGHT TO USE THE SOFTWARE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT.

1. Definitions

1.1. **Software** means software including any Updates and related materials.

1.2. **Rightholder** (owner of all rights, whether exclusive or otherwise to the Software) means Kaspersky Lab ZAO, a company incorporated according to the laws of the Russian Federation.

1.3. **Computer(s)** means hardware(s), including personal computers, laptops, workstations, personal digital assistants, 'smart phones', handheld devices, or other electronic devices for which the Software was designed where the Software will be installed and/or used.

1.4. **End User (You/Your)** means individual(s) installing or using the Software on his or her own behalf or who is legally using a copy of the Software; or, if the Software is being downloaded or installed on behalf of an organization, such as an employer, *"You"* further means the organization for which the Software is downloaded or installed and it is represented hereby that such organization has authorized the person accepting this agreement to do so on its behalf. For purposes hereof the term *"organization,"* without limitation, includes any partnership, li-

mited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

1.5. **Partner(s)** means organizations or individual(s), who distributes the Software based on an agreement and license with the Rightholder.

1.6. **Update(s)** means all upgrades, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance packs etc.

1.7. **User Manual** means user manual, administrator guide, reference book and related explanatory or other materials.

2. Grant of License

2.1. The Rightholder hereby grants You a non-exclusive license to store, load, install, execute, and display (to "use") the Software on a specified number of Computers in order to assist in protecting Your Computer on which the Software is installed, from threats described in the User Manual, according to the all technical requirements described in the User Manual and according to the terms and conditions of this Agreement (the "License") and you accept this License:

Trial Version. If you have received, downloaded and/or installed a trial version of the Software and are hereby granted an evaluation license for the Software, you may use the Software only for evaluation purposes and only during the single applicable evaluation period, unless otherwise indicated, from the date of the initial installation. Any use of the Software for other purposes or beyond the applicable evaluation period is strictly prohibited.

Multiple Environment Software; Multiple Language Software; Dual Media Software; Multiple Copies; Bundles. If you use different versions of the Software or different language editions of the Software, if you receive the Software on multiple media, if you otherwise receive multiple copies of the Software, or if you received the Software bundled with other software, the total permitted number of your Computers on which all versions of the Software are installed shall correspond to the number of licenses you have obtained from the Rightholder *provided* that unless the licensing terms provide otherwise, each purchased license entitles you to install and use the Software on such a number of Computer(s) as is specified in Clauses 2.2 and 2.3.

2.2. If the Software was purchased on a physical medium You have the right to use the Software for protection of such a number of Computer(s) as is specified on the Software package.

2.3. If the Software was purchased via the Internet You have the right to use the Software for protection of such a number of Computers that was specified when You purchased the License to the Software.

2.4. You have the right to make a copy of the Software solely for back-up purposes and only to replace the legally owned copy if such copy is lost,

destroyed or becomes unusable. This back-up copy cannot be used for other purposes and must be destroyed when you lose the right to use the Software or when Your license expires or is terminated for any other reason according to the legislation in force in the country of your principal residence or in the country where You are using of the Software.

2.5. You can transfer the non-exclusive license to use the Software to other individuals or legal entities within the scope of the license granted from the Rightholder to You provided that the recipient agrees to be bound by all the terms and conditions of this Agreement and substitute you in full in the license granted from the Rightholder. In case You fully transfer the rights granted from the Rightholder to use the Software You must destroy all copies of the Software including the back-up copy. If You are a recipient of a transferred license You must agree to abide by all the terms and conditions of this Agreement. If You do not agree to be bound by all the terms and conditions of this Agreement, You may not install and/or use the Software. You also agree as the recipient of a transferred license that You do not have any additional or better rights than what the original End User who purchased the Software from the Rightholder.

2.6. From the time of the Software activation or after license key file installation (with the exception of a trial version of the Software) You have the right to receive the following services for the defined period specified on the Software package (if the Software was purchased on a physical medium) or specified during purchase (if the Software was purchased via the Internet):

- Updates of the Software via the Internet when and as the Rightholder publishes them on its website or through other online services. Any Updates that you may receive become part of the Software and the terms and conditions of this Agreement apply to them;
- Technical Support via the Internet and Technical Support telephone hotline.

3. Activation and Term

3.1. If You modify Your Computer or make changes to other vendors' software installed on it, You may be required by the Rightholder to repeat activation of the Software or license key file installation. The Rightholder reserves the right to use any means and verification procedures to verify the validity of the License and/or legality of a copy of the Software installed and/or used on Your Computer.

3.2. If the Software was purchased on a physical medium, the Software can be used, upon your acceptance of this Agreement, for the period that is specified on the package commencing upon acceptance of this Agreement.

3.3. If the Software was purchased via the Internet, the Software can be used, upon your acceptance of this Agreement, for the period that was specified during purchase.

3.4. You have the right to use a trial version of the Software as provided in Clause 2.1 without any charge for the single applicable evaluation period (30 days) from the time of the Software activation according to this Agreement *provided that* the trial version does no entitle You Updates and Technical support via the Internet and Technical support telephone hotline.

3.5. Your License to Use the Software is limited to the period of time as specified in Clauses 3.2 or 3.3 (as applicable) and the remaining period can be viewed via means described in User Manual.

3.6. If You have purchased the Software that is intended to be used on more than one Computer then Your License to Use the Software is limited to the period of time starting from the date of activation of the Software or license key file installation on the first Computer.

3.7. Without prejudice to any other remedy in law or in equity that the Rightholder may have, in the event of any breach by You of any of the terms and conditions of this Agreement, the Rightholder shall at any time without notice to You be entitled to terminate this License to use the Software without refunding the purchase price or any part thereof.

3.8. You agree that in using the Software and in using any report or information derived as a result of using this Software, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, copyright, export control and obscenity law.

3.9. Except as otherwise specifically provided herein, you may not transfer or assign any of the rights granted to you under this Agreement or any of your obligations pursuant hereto.

4. Technical Support

The Technical Support described in Clause 2.6 of this Agreement is provided to You when the latest Update of the Software is installed (except for a trial version of the Software).
Technical support service: http://support.kaspersky.com

5. Limitations

5.1. You shall not emulate, clone, rent, lend, lease, sell, modify, decompile, or reverse engineer the Software or disassemble or create derivative works based on the Software or any portion thereof with the sole exception of a non-waivable right granted to You by applicable legislation, and you shall not otherwise reduce any party of the Software to human readable form or transfer the licensed Software, or any subset of the licensed Software, nor permit any third party to do so, except to the ex-

tent the foregoing restriction is expressly prohibited by applicable law. Neither Software's binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary. All rights not expressly granted herein are reserved by Rightholder and/or its suppliers, as applicable. Any such unauthorized use of the Software shall result in immediate and automatic termination of this Agreement and the License granted hereunder and may result in criminal and/or civil prosecution against You.

5.2. You shall not transfer the rights to use the Software to any third party except as set forth in Clause 2.5 of this Agreement.

5.3. You shall not provide the activation code and/or license key file to third parties or allow third parties access to the activation code and/or license key which are deemed confidential data of Rightholder and you shall exercise reasonable care in protecting the activation code and/or license key in confidence provided that you can transfer the activation code and/or license key to third parties as set forth in Clause 2.5 of this Agreement.

5.4. You shall not rent, lease or lend the Software to any third party.

5.5. You shall not use the Software in the creation of data or software used for detection, blocking or treating threats described in the User Manual.

5.6. The Rightholder has the right to block the key file or to terminate Your License to use the Software in the event You breach any of the terms and conditions of this Agreement and without any refund to You.

5.7. If You are using the trial version of the Software You do not have the right to receive the Technical Support specified in Clause 4 of this Agreement and You don't have the right to transfer the license or the rights to use the Software to any third party.

6. Limited Warranty and Disclaimer

6.1. The Rightholder guarantees that the Software will substantially perform according to the specifications and descriptions set forth in the User Manual *provided however* that such limited warranty shall not apply to the following: (w) Your Computer's deficiencies and related infringement for which Rightholder's expressly disclaims any warranty responsibility; (x) malfunctions, defects, or failures resulting from misuse; abuse; accident; neglect; improper installation, operation or maintenance; theft; vandalism; acts of God; acts of terrorism; power failures or surges; casualty; alteration, non-permitted modification, or repairs by any party other than Rightholder; or any other third parties' or Your actions or causes beyond Rightholder's reasonable control; (y) any defect not made known by You to Rightholder as soon as practical after the defect first appears; and (z) incompatibility caused by hardware and/or software components installed on Your Computer.

6.2. You acknowledge, accept and agree that no software is error free and You are advised to back-up the Computer, with frequency and reliability suitable for You.

6.3. The Rightholder does not provide any guarantee that the Software will work correctly in case of violations of the terms described in the User Manual or in this Agreement.

6.4. The Rightholder does not guarantee that the Software will work correctly if You do not regularly download Updates specified in Clause 2.6 of this Agreement.

6.5. The Rightholder does not guarantee protection from the threats described in the User Manual after the expiration of the period specified in Clauses 3.2 or 3.3 this Agreement or after the License to use the Software is terminated for any reason.

6.6. THE SOFTWARE IS PROVIDED "AS IS" AND THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY AS TO ITS USE OR PERFORMANCE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM THE EXTENT TO WHICH CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW THE RIGHTHOLDER AND ITS PARTNERS MAKE NO WARRANTY, CONDITION, REPRESENTATION, OR TERM (EXPRESS OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, SATISFACTORY QUALITY, INTEGRATION, OR APPLICABILITY FOR A PARTICULAR PURPOSE. YOU ASSUME ALL FAULTS, AND THE ENTIRE RISK AS TO PERFORMANCE AND RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, THE RIGHTHOLDER MAKES NO REPRESENTATION AND GIVES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET ANY OR ALL YOUR REQUIREMENTS WHETHER OR NOT DICLOSED TO THE RIGHTHOLDER .

7. Exclusion and Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE RIGHTHOLDER OR ITS PARTNERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR LOSS OF PRIVACY, FOR CORRUPTION, DAMAGE AND LOSS OF DATA OR PROGRAMS, FOR FAILURE TO MEET ANY DUTY INCLUDING ANY STATUTORY DUTY, DUTY OF GOOD

FAITH OR DUTY OF REASONABLE CARE, FOR NEGLIGENCE, FOR ECONOMIC LOSS, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SOFTWARE OR OTHERWISE ARISING OUT OF THE USE OF THE SOFTWARE, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, OR ARISING OUT OF ANY BREACH OF CONTRACT OR ANY TORT (INCLUDING NEGLIGENCE, MISREPRESENTATION, ANY STRICT LIABILITY OBLIGATION OR DUTY), OR ANY BREACH OF STATUTORY DUTY, OR ANY BREACH OF WARRANTY OF THE RIGHTHOLDER OR ANY OF ITS PARTNERS, EVEN IF THE RIGHTHOLDER OR ANY PARTNER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

YOU AGREE THAT IN THE EVENT THE RIGHTHOLDER AND/OR ITS PARTNERS ARE FOUND LIABILE, THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS SHALL BE LIMITED BY THE COSTS OF THE SOFTWARE. IN NO CASE SHALL THE LIABILITY OF THE RIGHTHOLDER AND/OR ITS PARTNERS EXCEED THE FEES PAID FOR THE SOFTWARE TO THE RIGHTHOLDER OR THE PARTNER (AS MAY BE APPLICABLE).

NOTHING IN THIS AGREEMENT EXCLUDES OR LIMITS ANY CLAIM FOR DEATH AND PERSONAL INJURY. FURTHER IN THE EVENT ANY DISCLAIMER, EXCLUSION OR LIMITATION IN THIS AGREEMENT CANNOT BE EXLUDED OR LIMITED ACCORDING TO APPLICABLE LAW THEN ONLY SUCH DISCLAIMER, EXCLUSION OR LIMITATION SHALL NOT APPLY TO YOU AND YOU CONTINUE TO BE BOUND BY ALL THE REMAINING DISCLAIMERS, EXCLUSIONS AND LIMITATIONS.

8. GNU and Other Third Party Licenses

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code ("Open Source Software"). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com or the source code is supplied with the Software. If any Open Source Software licenses require that the Rightholder provide rights to use, copy or modify an Open Source Software program that are broader than the rights granted in this Agreement, then such rights shall take precedence over the rights and restrictions herein.

9. Intellectual Property Ownership

9.1 You agree that the Software and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Software, are proprietary intellectual property and/or the valuable trade secrets of the Rightholder or its partners and that the Rightholder and its partners, as applicable, are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian Federation, European Union and the United States, as well as other countries and international treaties. This Agreement does not grant to You any rights to the intellectual property including any the Trademarks or Service Marks of the Rightholder and/or its partners ("Trademarks"). You may use the Trademarks only insofar as to identify printed output produced by the Software in accordance with accepted trademark practice, including identification of the Trademark owner's name. Such use of any Trademark does not give you any rights of ownership in that Trademark. The Rightholder and/or its partners own and retain all right, title, and interest in and to the Software, including without limitation any error corrections, enhancements, Updates or other modifications to the Software, whether made by the Rightholder or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software made hereunder must contain the same proprietary notices that appear on and in the Software. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Software and you acknowledge that the License, as further defined herein, granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement. Rightholder reserves all rights not expressly granted to you in this Agreement.

9.2 You acknowledge that the source code, activation code and/or license key file for the Software are proprietary to the Rightholder and constitutes trade secrets of the Rightholder. You agree not to modify, adapt, translate, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software in any way.

9.3 You agree not to modify or alter the Software in any way. You may not remove or alter any copyright notices or other proprietary notices on any copies of the Software.

10. Governing Law; Arbitration

This Agreement will be governed by and construed in accordance with the laws of the Russian Federation without reference to conflicts of law rules and prin-

ciples. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. Any dispute arising out of the interpretation or application of the terms of this Agreement or any breach thereof shall, unless it is settled by direct negotiation, be settled by in the Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry in Moscow, the Russian Federation. Any award rendered by the arbitrator shall be final and binding on the parties and any judgment on such arbitration award may be enforced in any court of competent jurisdiction. Nothing in this Section 10 shall prevent a Party from seeking or obtaining equitable relief from a court of competent jurisdiction, whether before, during or after arbitration proceedings.

11. Period for Bringing Actions.

No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

12. Entire Agreement; Severability; No Waiver.

This Agreement is the entire agreement between you and Rightholder and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Software or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Rightholder provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Rightholder's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

13. Contact Information.

Should you have any questions concerning this Agreement, or if you desire to contact the Rightholder for any reason, please contact our Customer Service Department at:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscow, 123060
Russian Federation
Tel: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Web site: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. All Rights Reserved. The Software and any accompanying documentation are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.